AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An apparatus for managing access to a resource over a network, comprising:

a receiver arranged to receive a request for access to the resource from a client device; and

a policy manager, coupled to the receiver, that is arranged to perform actions, including:

~~determining a configuration of the client device;~~

downloading a component onto the client device, wherein the downloaded component is configured to inspect the client device to detect a configuration of the client device;

receiving from the downloaded component the configuration of the client device based on the inspection;

applying a dynamic policy for the access based, in part, on the received ~~determined~~ configuration; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

2. (Currently Amended) The apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to not download the component, then receiving the configuration of the client device through a browser residing on the client device. ~~receive a downloadable component, providing the downloadable component to the client device.~~

3. (Currently Amended) The apparatus of claim 1, wherein the received configuration indicates whether the client device is operating as a kiosk. ~~2, wherein the downloadable component is configured to inspect an environment of the client device and provide environment information to the policy manager.~~

4. (Original) The apparatus of claim 1, wherein determining the configuration of the client device further comprises determining information associated with the connection between the client device and the resource.

5. (Currently Amended) The apparatus of claim 1, wherein inspecting the client device to detect a configuration further comprises detecting if security software is installed on the client device and if security software is installed, inspecting the security software to detect if the security software is active or disabled. ~~further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.~~

6. (Original) The apparatus of claim 1, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

7. (Original) The apparatus of claim 1, wherein the restriction includes at least one downloadable component.

8. (Original) The apparatus of claim 1, wherein the restriction is configured to intercept a communication between the client device and the apparatus.

9. (Original) The apparatus of claim 1, wherein applying the restriction further comprises performing at least one of intercepting a system command, inhibiting a file save, inhibiting a file print, restricting launching of a predetermined application, and redirecting access to a file.

10. (Currently Amended) A method of managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

~~determining a configuration of the client device;~~

downloading a component onto the client device, wherein the downloaded component is configured to inspect the client device to detect a configuration of the client device;

receiving from the downloaded component the configuration of the client device based on the inspection;

applying a dynamic policy for the access based, in part, on the received ~~determined~~ configuration; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

11. (Original) The method of claim 10, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.

12. (Currently Amended) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating whether the client device is a laptop, personal computer, kiosk, or a mobile device. ~~determining the configuration further comprises, if the client device is configured to receive a downloadable component, providing the downloadable component to the client device, wherein the downloadable component is configured, in part, to determine the configuration of the client device.~~

13. (Currently Amended) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating ~~determining the configuration further comprises determining~~ at least one of one level of trust associated with the client device, a type of encryption enabled on the client device, a type of antivirus enabled on the client device, a security feature enabled on the client device, a browser type, an operating system configuration, a security certificate, and if a hacker tool is enabled on the client device.

14. (Currently Amended) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating ~~determining the configuration further comprises determining~~ a level of trust of the client device.

15. (Currently Amended) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating ~~determining the configuration further comprises determining~~ a characteristic of an enabled security application enabled.

16. (Original) The method of claim 10, wherein applying the restriction further comprises downloading a component to the client device.

17. (Original) The method of claim 10, wherein applying the restriction further comprise configuring a virtual sandbox to intercept a communication between the client device and the resource.

18. (Original) The method of claim 17, wherein intercepting the communication further comprises blocking a download of at least one file to the client device.

19. (Original) The method of claim 10, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command.

20. (Original) The method of claim 10, wherein applying the dynamic policy further comprises determining at least one of a connector, and an adaptor to enable the access to the resource.

21. (Original) The method of claim 10, wherein applying the dynamic policy further comprises restricting the access to the resource.

22. (Currently Amended) A network appliance for managing access to a resource over a network, comprising:

a transceiver for receiving a request for access to the resource from a client device; and

a processor that is configured to perform actions, including:

receiving the request for access;

~~determining a configuration of the client device;~~

downloading a component onto the client device, wherein the downloaded component is configured to inspect for a configuration of the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection;

applying a dynamic policy for the access based, in part, on the received ~~determined~~ configuration; and

applying a restriction to the access for the requested resource, wherein the restriction is configured based on the applied dynamic policy.

23. (Currently Amended) The network appliance of claim 22, wherein the processor is configured to perform further actions, comprising: in response to receiving the request for access to the resource, receiving additional information about the configuration of the client device through a query with a browser residing on the client device. ~~transmitting a downloadable component to the client device.~~

24. (Original) The network appliance of claim 22, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

25. (Currently Amended) The network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is not configured to receive a downloadable component, receiving information about the configuration of the client device through a browser application residing within the client device. ~~providing the downloadable component to the client device.~~

26. (Original) The network appliance of claim 22, wherein applying the dynamic policy further comprises:

if the client device is configured to restricting a download of a component, restricting access to the resource.

27. (Original) The network appliance of claim 22, wherein applying the restriction further comprises:

if the client device is configured to restrict a download of a component, intercepting a communication between the client device and the requested resource to perform at least one of preventing an access to file, and restricting an action.

28. (Currently Amended) A ~~modulated data signal~~ computer readable storage medium that includes data and instructions, wherein the execution of the instructions on a computing device provides for managing access to a resource over a network by enabling actions, comprising:~~, the modulated data signal comprising the actions of:~~

receiving a request for access to the resource from a client device;

~~sending a configuration of the client device;~~

downloading a component onto the client device, wherein the downloaded component is configured to inspect for a configuration of the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection;

applying a dynamic policy to the access based, in part, on the ~~sent~~ configuration of the client device; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

29. (Currently Amended l) The computer readable storage medium ~~modulated data signal~~ of claim 28, wherein applying the restriction further comprises configuring a virtual sandbox to intercept a communication between the client device and the resource.

30. (Currently Amended) The computer readable storage medium ~~modulated data signal~~ of claim 28, wherein applying the restriction further comprises blocking a download of at least one file to the client device.

31. (Currently Amended) An apparatus for managing access to a resource over a network, comprising:

a transceiver arranged to receive a request for access to the resource from a client device; and

a policy manager, coupled to the transceiver, that is arranged to perform actions, including:

~~a means for determining a configuration of the client device;~~

downloading a component onto the client device, wherein the downloaded component is configured to inspect the client device to detect a configuration of the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection, wherein the configuration includes at least an indication of a status of an security application residing on the client device including whether the application is active or disabled;

~~a means for~~ applying a dynamic policy for the access based, in part, on the ~~determined~~ configuration; and

~~a means for~~ restricting to the access for the requested resource, wherein the means for restricting is configured based, in part, on the applied dynamic policy.

32. (Original) A method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining a level of security software enabled on the client device;

applying a dynamic policy to the access based, in part, on the determined level of security software enabled; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

33. (Currently Amended) A method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining if the client device is configured as a kiosk or a mobile device ~~a configuration of an operating system active on the client device~~; and

applying a restriction to the access for the requested resource based on the determined configuration of the client device ~~operating system~~.

34. (Canceled)